Extended DRI Table Detection Method for Gray Hole

[1]Amarjit Malhotra , [1]Abhishek Patro, [1]Deepika Anand,
[1]Division of Information Technology, Netaji Subhash Institute of Technology New Delhi 110075, INDIA
uppalz_amar@yahoo.com,agbpatro@gmail.com, deepika_087@yahoo.com

Abstract-**The MANET (Mobile Adhoc network) consists of mobile nodes. This feature along with undefined and unsecure boundaries makes its security a very challenging issue. One such issue is the gray hole attack. The Gray hole FALSELY SELECTIVELY advertises itself to be having the shortest route to the destination and when route is established, it selectively starts dropping packets. The extent of dropping packets is decided by the gray magnitude of the node. In this paper we suggest a mechanism to detect the gray hole on AODV protocol in MANET using a Extended Data Routing Information (EDRI) table in addition to existing routing tables at each node. This mechanism helps in detection of gray holes and thereby discouraging any route formation via the gray hole. Simulation proves that this method is a pertinent algorithm to detect gray holes in moderate and high data traffic.**

Keywords – Adhoc, EDRI table, Gray magnitude, Gray Hole, MANETS

1 Introduction

A Mobile Ad hoc NETwork MANET is a group of mobile nodes that cooperate and forward packets for each other [3]. Such a network is well suited in scenarios where there is no central controlling system. As for a small scale project, it is not advisable to set up an infrastructure for networking. MANETS have special characteristics such as dynamic topology, battery life constraints, limited bandwidth, and unreliable links among the nodes. While these characteristics help in the flexibility of networks but introduce various attacks [8] such as Sybil attack, Rushing attack, Wormhole attack, Blackhole attack, Grayhole attack etc., which makes such networks unreliable. Since nodes in an ad hoc network also function as routers that discover and maintain routes to other nodes in the network, if routing is misdirected or even worse dropped, the entire network will be paralyzed. In this paper, we concentrate on prevention of the Grayhole attack by malicious nodes.

In a Grayhole attack, a node selectively drops packets and forwards the rest. A similar kind of attack is a blackhole attack in which all packets received are dropped by the malicious node.

In this paper, we propose an innovative approach to detect gray hole attack by maintain an **EDRI** (Extended Data Routing Information) table at each node. The fields of this table are used to detect a malicious node as well as maintain a history of previously detected malicious nodes.

The rest of this paper is outlined as follows.

2 Related Work

A number of mechanisms have been proposed earlier for mitigation of attacks by malicious nodes and to deliver data securely.

S. MARTI et al[1] proposed detection of malicious nodes using watchdog/pathrater mechanism. This scheme can be divided into parts **1) Detection:** Each node in the route has a monitoring node known as the watchdog. This node promiscuously hears the next node's transmissions. The suspicion level is increased for each failed transmission and on reaching the threshold limit it broadcasts the information of being a black hole to the source node. **2) Mitigation:** The source node selects the best available path according to the information present in the network. In pathrater each node uses the watchdog's monitered results to rate its one hop neighbours. Further the nodes exchange their ratings. However, this mechanism has certain drawbacks.

The algorithm is fails to detect collision among the nodes(secondly to detect behaviour of node two or three hops away ,one node has to trust another node which introduces vulnerability as good nodes may be bypassed by malicious accusation)

J. SEN et al [5] proposed a mechanism to detect a gray hole using probe packet and DRI table. Global alarming a digitally signed message requires atleast k nodes. The drawback of this algorithm is that if a gray hole is in a sparse area, it cannot be detected as min k no of nodes are required to sign an alarm message.

CAI et al [3] proposed a mechanism of detecting a black and gray hole by modifying the detecting threshold according to the network's overload .The algorithm makes use of FwdPktBuffer and dynamic threshold. The detecting node can only accuse a node of being a gray hole when it overhears the next hops "drops" packets in probability higher than the dynamic threshold value. The algorithm suffers from a drawback that when collision rate increases, dynamic threshold increases as well therefore gray hole may not be detected.

Ramaswamy et al [7] proposed a methodology for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking. The solution to identify multiple black hole nodes acting in cooperation is done effectively by adding additional control packets. The neighbour node is then checked for its malicious activity by cross-checking with its own DRI table. This cross checking loop will be

continued until a trusted node is found. The solution fails to accommodate the Grayhole Attack where the nodes keep alternating between malicious and normal behaviour.
In this paper, we propose a methodology for identifying gray-hole nodes with slightly modified AODV protocol by extending the DRI Table.
Less overheads are involved in our approach as minimal control packets have been used to detect the malicious node.

3 Gray Hole Attack

AODV protocol[4] are vulnerable to a number of attacks. We will first describe the protocol itself and then analyse one such vulnerability known as gray-hole attack. When source node (SN) wishes to send data to a destination node (DN), it broadcasts a Route-Request (RREQ) packet to its immediate neighbours. Upon receiving a RREQ packet, the nodes update their route tables for reverse route to the source node and also increase the hop-count of the packet. These nodes then re-broadcast the packet if they do not have a known route to the destination. A Route-Reply (RREP) packet is then sent back to the source node by an intermediate node having a known route to the destination or by the destination itself.

A Gray-hole attack is possible when the distance between source and destination is more than 2-3 hops. The attack can initiate at different phases of information routing. 1) A malicious node (GN) can intercept data by falsely advertising itself of having a known route to the destination during the route initiation phase. **Figure a** illustrates this kind of attack. Source Node (SN) will accept the fake reply by GN as it promises fresh enough route with least hop count. 2) Another method is to behave normally during route initiation phase and drop packets when a route is formed with itself as an intermediate node. **Figure z** illustrates this kind of attack.

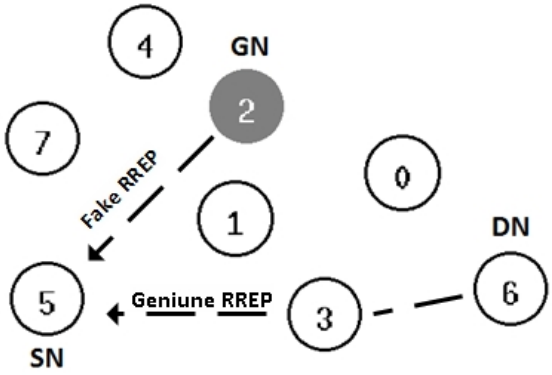


Figure a Attack during route initiation

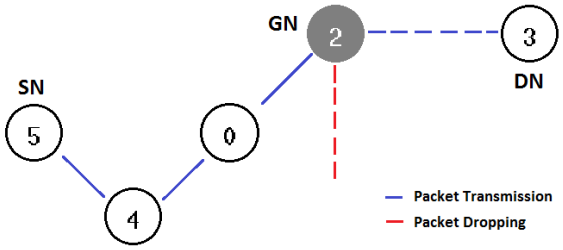


Figure z Attack during data transmission

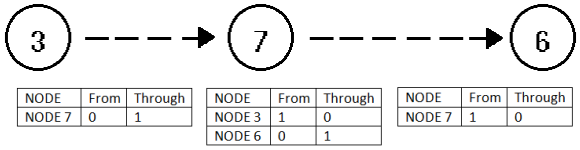
The second method is an effective method to successfully infiltrate a network since it is difficult to detect**.** In fig/case a 1.)GN can be detected by time interval method as the malicious node does not need to check its routing table for the existence of valid path. The response from malicious node is likely to be received first[9] 2.)By comparing the sequence number of RREP from destination and GN. 3.) By comparing the difference in number of hops of RREP given by GN and other routes from destination.

4 Proposed Approach

In this section , we propose our methodology by first discussing the DRI Table[7] for the completion purpose . For identifying a Gray Hole we have extended DRI as discussed later.

4.1 DRI TABLE

Each node maintains an additional table known as Data Routing Information (DRI) table. In the DRI table, 1 stands for 'true' and 0 for 'false'.



NODE	From	Through
NODE 7	0	1

NODE	From	Through
NODE 3	1	0
NODE 6	0	1

NODE	From	Through
NODE 7	1	0

Figure X Data routing from node 3 to node 6

The first bit "**From**" is set for those nodes in the table who send data to it while the second bit "**Through**" stands for information on routing data packet through the node i.e. it is set for those nodes in the table when the next node forwards the data sent by it.
In figure X, the DRI table of node 6 has set from value for node 7 since it has successfully received data and DRI table of node 3 has set through value for node 7 since node 7 forwards the data to node 6.

4.2 EDRI TABLE

In addition to the original DRI table, we have proposed to add a set of new attributes in the table for detection of grayholes. They are as follows:-
i) FTS (From Time Stamp):- This field is set to the time when the from field for a particular node of the DRI table is being recorded for the first time.
ii) UFTS (Updated FTS):-This field contains the most updated time stamp when the from field for a particular node of the DRI table is updated.

iii) TTS (Through Time Stamp):- This is field is set to the current time when the through field for a particular node of the DRI table is being recorded for the first time.
iv) UTTS (Updated TTS):- This field contains the most updated time stamp when the through field for a particular node of the DRI table is updated.
v) FromCounter:- This fields increments its value every time the from field of a particular node is updated.
vi) ThroughCounter:- This fields increments its value every time the through field of a particular node is updated.
vii) WhiteMagnitude (wm):- This field records the malicious behaviour of its neighbour nodes. Its value lies in the range of 0 to 1 with zero being a BLACK hole and 1 being a WHITE hole. Any intermediate value tells us that the node is GRAY in nature. It is initialized as 1.
Note that the malicious activity, i.e. GrayMagnitude(gm) is given by:-

$$gm = (1- wm)$$

4.3 METHODOLOGY FOR THE PROPOSED TECHNIQUE

In order to prevent attack by malicious nodes, our approach aims at providing mitigation techniques at route initiation phase and data transmission phase.

4.3.1 PREVENTION OF ATTACK AT ROUTE INITIATION PHASE

Malicious nodes may or may not generate fake RREP packet on detecting a RREQ packet in the network. These fake responses can be detected by incorporating additional control packets and modifying the RREP packet which is analogous to the approach given by [7]. RREP packet should have an additional field NEXT HOP (NH), which contains the node address to whom the data will be transmitted to and null if RREP is sent by the destination node (DN). The packet should also have DRI entries for the node NH. Upon receiving a RREP response from an intermediate node (IN), the source node (SN) sends a Further Request (FREQ) packet to node NH through an alternate route not having IN. The FREQ asks NH to provide its DRI entries for the node IN. NH then sends a Further Reply (FREP) packet to SN containing the DRI entries of IN. The whole mechanism is illustrated in **Figure y** and **Figure z**.

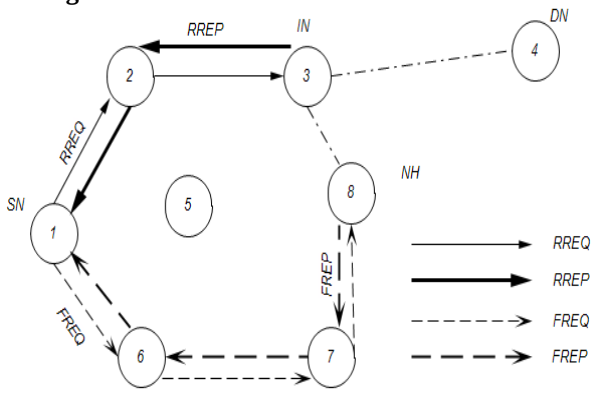


Figure Z Seq. Diagram of Route Formation

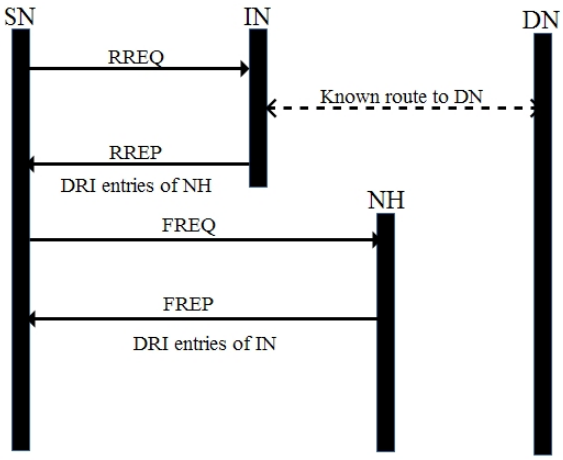


Figure Z Seq. Diagram of Route Formation

When the SN has obtained DRI entries from both IN and NH, it can determine whether the RREP generated was fake or genuine. If the response was faked, SN raises a global alarm in the network exposing maliciousness of IN.

4.3.2 PREVENTION OF ATTACK DURING DATA TRANSMISSION PHASE

If the gray node behaves normally during the first phase and then starts dropping packets selectively after the route has successfully been established, then the following detection algorithm can used to detect malicious nodes.
Whenever an intermediate node receives data from its neighbours, it checks its EDRI entries for following factors before updating its fields:-
1) Is this the first time neighbour node has sent data for this route?
2) When was the last time the data was received from the same neighbour node?
3) Is the neighbour a registered malicious node?
In addition to this the IN starts a timer for its previous hop. If timeout occurs, the malicious activity is increased for the previous node in the EDRI table by the procedure mentioned later in this section.
Upon receiving data for the first time, the white magnitude (wm) is unaffected (it remains 1). Upon receiving subsequent data packets, a new white magnitude (nwm) for the previous hop (PH) is computed as follows (assume CTS as current timestamp):-

1) If (CTS-UFTS) < 1.5*interval, nwm is set to 1.
2) Else if (CTS-UFTS) < 2.3*interval, nwm is set to 0.5.
3) Else if (CTS-UFTS) < TimeoutTime, nwm is set to 0.3.
4) Else, for the case if (CTS-UFTS) >= TimeoutTime, wm is computed given later in this section.

The resultant wm is computed as a weighted sum of nwm and the old white magnitude (owm) maintained by the EDRI table which is given by:-

$$wm = \frac{\alpha * (UFTS - FTS) * owm + \beta * (CTS - UFTS) * nwm}{\alpha * (UFTS - FTS) + \beta * (CTS - UFTS)}$$

α and β are we weightage given to the old and new white magnitude respectively.

Note that:-

$$\alpha + \beta = 1$$

Apart from the above conditions, if a timeout occurs then the wm is given by:-

$$wm = 0.9 * owm$$

and the timer is started again till the lifetime is valid.

A repeated and consecutive series of timeout will decrement the wm below the threshold value and a global alarm will be raised and will not be used in future for establishing routes. **Figure tt** illustrates this phase of detection for the route formed in **figure x.**

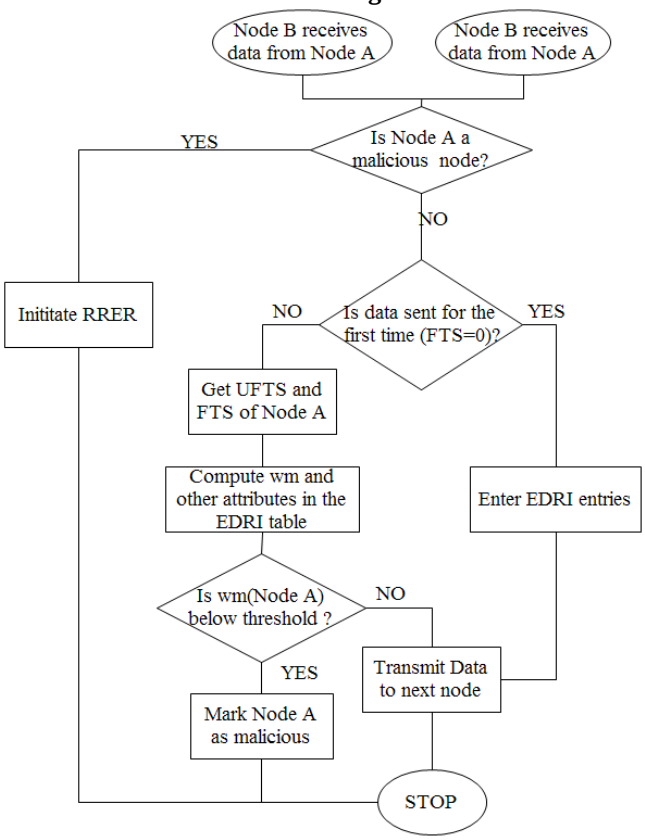


Figure tt prevention of attack during data transmission phase

Also, before transmitting data to its next hop, it starts a timer for the next hop and a new white magnitude (nwm) for the NH is computed as follows on similar basis as discussed previously

1) If (CTS-UTTS) < 1.5*interval, nwm is set to 1.
2) Else if (CTS-UTTS) < 2.3*interval, nwm is set to 0.5.
3) Else if (CTS-UTTS) < TimeoutTime, nwm is set to 0.3.
4) Else, for the case if (CTS-UTTS) >= TimeoutTime, wm is computed by:-

$$wm = 0.9 * owm$$

Therefore, a single IN computes wm for PH and NH. **Figure uu** illustrates this phase of detection for the route formed in **figure x**.

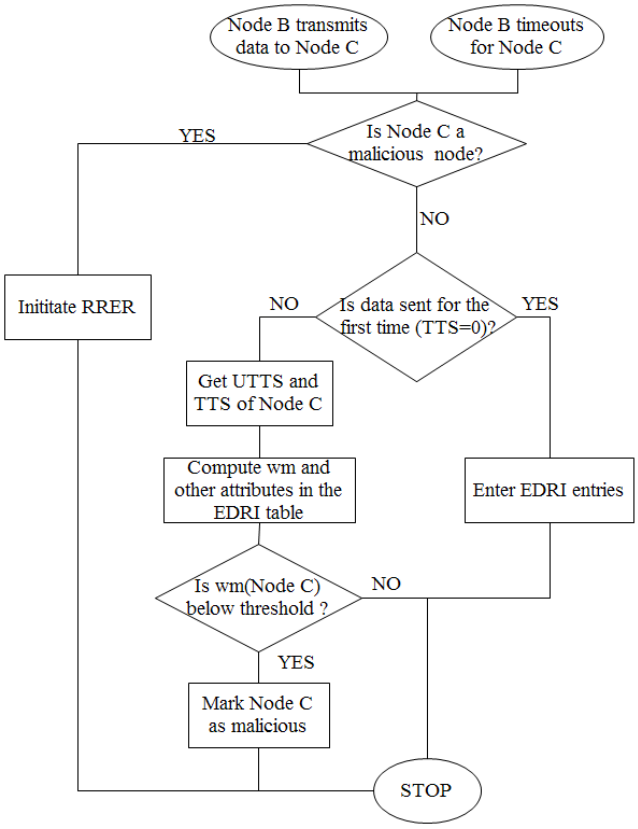


Figure uu prevention of attack during data transmission phase

When a node (acting as a source node) wants to establish a route in future, it can select the best available neighbour according to the value of wm which it receives from the RREP and FREP packets and may also be stored in its EDRI table respectively.

4.4 ANALYSIS OF THE FORMULA

Let us assume:-

$$F1 = \frac{\alpha * (UFTS - FTS) * owm}{\alpha * (UFTS - FTS) + \beta * (CTS - UFTS)}$$

$$F2 = \frac{\beta * (CTS - UFTS) * nwm}{\alpha * (UFTS - FTS) + \beta * (CTS - UFTS)}$$

Figure aa plots a sample simulation data for a particular node which was activated for about 110 seconds and shows the relation between F_1 with time(t), F_2 with time(t) and finally weightage of F_1 and F_2 in finding out the resultant wm over the period of time.

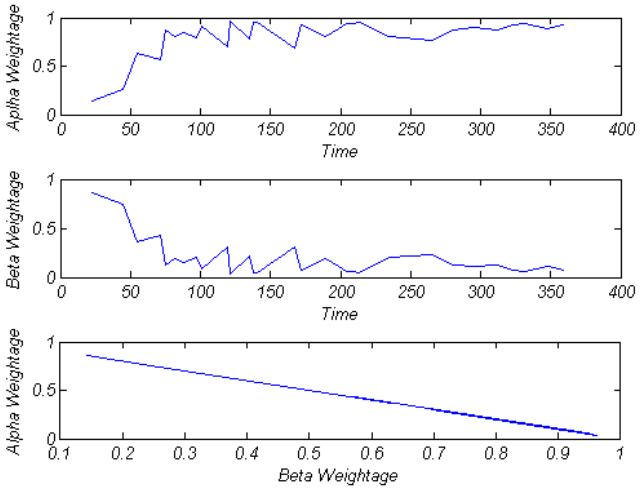


Figure aa Mathematical Relations

The weightage of nwm and owm is dependent on the following two factors:-

1) Time

Initially, the owm provided by F_1 is given lesser weightage than that of nwm in F_2 since relative new data would be more accurate than the old data. As time increases the period of time, weight of F_1 gradually increases and that of F_2 decreases since owm is becoming consistent due to the factor that it was calculated over the period of time while nwm was calculated for very short period.

2) The constants, α and β

When the node is active for large period of time, the value given by F_2 will become insignificant if proper measures are not taken in calculating resultant wm. Therefore for proper interpolation, the value of constant α is kept lesser than that of β. Usually α is equal to 0.3 while β is equal to 0.7(1-0.3).

5 Simulation and results

5.1 Simulation

The proposed mechanism is simulated and tested in Global Network Simulator (GlomoSim version 2.03)[6] for the purpose of evaluation and performance. The simulation environment was as follows:-

Parameters	Values
Physical Layer	**UNDECIDED**
Mac Layer	802.11
Routing Protocol	AODV
Network Protocol	IP addressing
TCP Protocol	UDP

The terrain dimensions were 1500*1500 m^2 and 30 nodes were uniformly placed all over the region. At application layer CBR was used and we sent packets of size 512 bytes from source to destination at different intervals. The network was simulated for **X seconds**. Nodes were moving according to random waypoint model and its effects were recorded at variable speeds.

5.2 Results

The criteria for evaluating the mechanisms were according to following parameters. 1) Detection Ratio: Ratio of total number of malicious nodes detected to the number of malicious nodes present in the network. 2) False Probability: Ratio of accounting non-malicious nodes as malicious to the total number of malicious nodes detected. 3) Packet delivery ratio: Percentage of data successfully delivered.

6 Conclusion and future work

In this paper, we have presented a mechanism for detection of malicious gray holes in MANETs. Due to their interchangeable behaviour between black and white, gray holes are very difficult to detect. The proposed mechanism increases the detection probability by using data from neighbor nodes instead of largely depending on control packets thus reducing any discrepancies in the data. The calculation of gray magnitude is also dynamic thereby providing optimal results. Since we have used rudimentary mathematics in calculating gray-magnitude, we can even use higher order mathematics to get even better results. The future work includes modification to the proposed mechanism to extend it for colluding (co-operative) gray holes. The simulation results show that the current mechanism adopted is efficient with low false positive rate and minimal control overhead.

7 References

[1] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of the Sixth Annual ACM/IEEE International Conference on MOBICOM, August 2000.

[2] Gao Xiaopeng, Chen Wei.A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks in IFIP International Conference on Network and Parallel Computing ,2007.

[3] Jiwen Cai, Ping Yi, Jialin Chen, Zhiyang Wang, Ning Liu. An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network in 24th IEEE International Conference on Advanced Information Networking and Applications,2010.

[4] Mobile Ad Hoc Networking Working Group. Internet Draft.

[5] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar in A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks in International Conference on Information,Communications and Signal Processing 2007

[6] Xiang Zeng, RajiveBagrodia, Mario Gerla,"GloMoSim: a Library for Parallel Simulation of Large-scale Wireless Networks", Proceedings of the 12th Workshop on Parallel and Distributed Simulations – PADS '98, May 26-29, 1998.

[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003.

[8] Ad Hoc Mobile wireless Networks: Protocols and Systems by C.K. Toh.

[9] Routing Security in Wireless Ad Hoc Networks Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati]